CLAIMS

1. **(Currently Amended)** A method comprising:

creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key and a keyed-hash message authentication code encrypted using a hash of a password associated with the user ID, wherein the data structure comprises a plurality of different encryptions of the master key such that the master key may be obtained by operation of any of a plurality of different keys, and each of the plurality of different encryptions is associated with a different user from among ~~one of~~ the plurality of users, respectively, and wherein a data integrity verification feature, comprising the keyed-hash message authentication code, is based on the hash of the password and is added to each of the plurality of different encryptions of the master key;

checking integrity of user keys from the plurality of user id-user key pairs after each of the plurality of user keys is produced, wherein the integrity check comprises decrypting the user key for comparison to the master key;

storing data ~~watermarked~~ encrypted using the master key;

receiving a user id and user password from one of the plurality of users;

selecting a user key from the data structure based on the received user id;

preventing fraudulent access to data comprising: tracking attempts by a user to access data, and blocking attempts for a time period after a threshold number of failed attempts; reporting failed data access attempts to a system administrator according to

user ID; increasing a time period a user must wait to attempt to access data after successive failed attempts to access the data; and, deleting a user ID and a user key after a threshold number of failed attempts to access data;

hashing the received password to produce a hash value;

decrypting the selected user key using the hash value to reproduce the master key; and

decrypting the stored data using the master key ~~to access the watermarked data; and~~

~~delivering the data structure to one or more of the plurality of users~~.

2. (Currently Amended) A method as recited in claim 1, ~~wherein the act of delivering comprises~~ additionally comprising delivering the data structure to each of the plurality of users.

3. (Cancelled)

4. (Previously Presented) A method as recited in claim 1, wherein the master key is encrypted using a one-way hash of the password associated with the one of the plurality of users.

5. (Previously Presented) A method as recited in claim 1, wherein the master key is encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

6. (Original) A method as recited in claim 1, wherein each user key has an integrity verification feature associated therewith.

7. (Previously Presented) A method as recited in claim 1, wherein the master key has an integrity verification feature associated therewith.

8. (Previously Presented) A method as recited in claim 1, wherein each master key and each user key has an integrity verification feature associated therewith.

9. (Original) A method as recited in claim 1, wherein each user key includes a checksum.

10. (Cancel)

11. (Currently Amended) A method as recited in claim 1, further comprising: ~~transforming~~ encrypting data using the master key.

12-16. (Cancelled)

17. (Withdrawn) A method comprising:

retrieving a user key associated with a first user of a plurality of users from a data structure comprising a plurality of user keys, each user key comprising a master key encrypted using a password associated with a unique one of the plurality of users;

decrypting the retrieved user key using a password associated with the first user to produce a master key; and

accessing data using the master key.

18. (Withdrawn) A method as recited in claim 17, wherein the user key is retrieved using a user id associated with the first user.

19. (Withdrawn) A method as recited in claim 17, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users.

20. (Withdrawn) A method as recited in claim 17, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users, and wherein the user key is retrieved using a user id associated with the first user.

21. (Withdrawn) A method as recited in claim 17, wherein the act of decrypting the user key comprises decrypting the user key using a hash of the password associated with the first user.

22. (Withdrawn) A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user to produce a hash value; and

using the hash value as a decryption key to decrypt the user key.

23. (Withdrawn) A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a one-way hash function; and

using the result of the one-way hash function as a decryption key to decrypt the user key.

24. (Withdrawn) A method as recited in claim 17, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a cryptographic hash function; and

using the result of the cryptographic hash function as a decryption key to decrypt the user key.

25. (Withdrawn) A method as recited in claim 17, wherein each of the plurality of user keys includes a data verification feature.

26. (Withdrawn) A method as recited in claim 17, wherein each of the plurality of master keys includes a data verification feature.

27. (Withdrawn) A method as recited in claim 17, further comprising:

verifying the integrity of the retrieved user key.

28. (Withdrawn) A method as recited in claim 17, wherein the retrieved user key includes an integrity verification feature and wherein the method further comprises verifying the integrity of the retrieved user key using the integrity verification feature.

29. (Withdrawn) A method as recited in claim 17, wherein the retrieved user key includes a checksum and wherein the method further comprises verifying the integrity of the retrieved user key using the checksum.

30. (Withdrawn) A method as recited in claim 17, wherein the retrieved user key includes a message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the message authentication code.

31. (Withdrawn) A method as recited in claim 17, wherein the retrieved user key includes a keyed-hash message authentication code and wherein the method

further comprises verifying the integrity of the retrieved user key using the keyed-hash message authentication code.

32-39. (Cancelled)

40. (Withdrawn) A system comprising:

a hashing module operable to hash each of a plurality of user passwords to produce a plurality of hash values;

an encryption module operable to create a plurality of user keys, each user key comprising a master key encrypted using one of the hash values as an encryption key; and

a data structure creation module operable to associate each of the user keys with a user id in a data structure.

41. (Withdrawn) A system as defined in claim 40, wherein the hashing module produces the hash values using a one-way hashing function.

42. (Withdrawn) A system as defined in claim 40, wherein the hashing module produces the hash values using a cryptographic hashing function.

43. (Withdrawn) A system as defined in claim 40, wherein the data structure creation module associates each user key with a user id in a user id-user key pair, and wherein each user id-user key pair is associated with a single user.

44. (Withdrawn) A system as defined in claim 40, wherein the encryption module includes an integrity verification feature in each user key.

45. (Withdrawn) A system as defined in claim 40, wherein the encryption module includes a checksum in each user key.

46. (Withdrawn) A system as defined in claim 40, wherein the encryption module includes a message authentication code in each user key.

47. (Withdrawn) A system as defined in claim 40, wherein the encryption module includes a keyed-hash message authentication code in each user key.

48. (Withdrawn) A system comprising:

a user key data structure including plurality of user id-user key pairs, each user key pair including a user key and a user id associated with one of a plurality of users, each user key comprising an encrypted version of a common master key;

a master key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using a password received from the one of the plurality of users.

49. (Withdrawn) A system as recited in claim 48, further comprising a data decryption module operable to decrypt data encrypted using the master key as an encryption key.

50. (Withdrawn) A system as recited in claims 48, further comprising an error handler module operable to indicate to the one of the plurality when an error occurs in decrypting the user key.

51. (Withdrawn) A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

52. (Withdrawn) A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users using a one-way hashing function to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

53. (Withdrawn) A system as recited in claim 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users using a cryptographic hashing function to produce a hash value; and

a user key decryption module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users and to decrypt the selected user key using the hash value as a decryption key.

54. (Withdrawn) A system as recited in claims 48, wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption and integrity module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users, to confirm the integrity of the selected user id, and to decrypt the selected user key using the hash value as a decryption key.

55. (Withdrawn) A system as recited in claims 48, wherein each user key in the user key data structure includes an integrity verification feature, and wherein the master key decryption module comprises:

a hashing module operable to hash a password received from the one of the plurality of users to produce a hash value; and

a user key decryption and integrity module operable to select a user key from the user key data structure based on a user id received from one of the plurality of users, to confirm the integrity of the selected user id using the integrity verification feature included in the user key, and to decrypt the selected user key using the hash value as a decryption key.

56. (Currently Amended) A system comprising:

means for producing a plurality of user keys, wherein each user key is associated with one of a plurality of users, respectively, and wherein each of the plurality of user keys ~~is~~ comprises a different ~~an~~ encryption of a single master key, and wherein ~~the~~ each different encryption is performed by operation of a reversible process using a hash value of a ~~different~~ password associated with each user as a key in the reversible process, and wherein each user key additionally comprises a keyed-hash message authentication code encrypted using the hash value of the password associated with the user;

means for checking integrity of the plurality of user keys after each of the plurality of user keys is produced, wherein the integrity check comprises decrypting the user key for comparison to the master key;

means for storing a plurality of user IDs, wherein each user ID is associated with one of a plurality of user keys within a user key data structure, and wherein the user key data structure is configured to provide a user key in response to input of a user ID;

means for storing encrypted data using the master key;

means for accessing, upon presentation of a user ID of a user, a user key associated with the user ID of the user, wherein the accessing is from the user key data structure;

means for hashing, upon presentation of a password of the user, the presented password to produce a hash value;

means for verifying the keyed-hash message authentication code encrypted using the hash of the password associated with the user;

means for decrypting the user key using the hash value, thereby creating the master key;

means for preventing fraudulent access to data comprising: tracking attempts by a user to access data, and blocking attempts for a time period after a threshold number of failed attempts; reporting failed data access attempts to a system administrator according to user ID; increasing a time period a user must wait to attempt to access data after successive failed attempts to access the data; and, deleting a user ID and a user key after a threshold number of failed attempts to access data; and

means for decrypting data using the master key.

57. (Currently Amended) A computer-readable medium having stored thereon computer executable instructions for performing acts of:

storing data encrypted with a master key;

creating a data structure comprising a plurality of user keys paired with user IDs, wherein each user key is associated with one of a plurality of users, respectively, and wherein each of the plurality of user keys ~~is~~ comprises a different ~~an~~ encryption of a ~~single~~ the master key, encrypted by operation of a reversible process using a hash value of a password associated with user, and wherein each user key additionally comprises a keyed-hash message authentication code encrypted using the hash value of the password associated with the user;

accessing, upon presentation of a user ID of a user, a user key associated with the user ID, from the data structure;

hashing, upon presentation of a password of the user, the presented password to produce a hash value;

preventing fraudulent access to data comprising: tracking attempts by a user to access data, and blocking attempts for a time period after a threshold number of failed attempts; reporting failed data access attempts to a system administrator according to user ID; increasing a time period a user must wait to attempt to access data after successive failed attempts to access the data; and, deleting a user ID and a user key after a threshold number of failed attempts to access data;

verifying the keyed-hash message authentication code encrypted using the hash of the password associated with the user;

decrypting the user key using the hash value, thereby creating the master key;

decrypting data using the master key; and

sending the data to the user.

58. (Original) A computer-readable medium as recited in claim 57 having further computer executable instructions for performing acts of:

delivering the data structure to one or more of the plurality of users.

59-71. (Cancelled).

72. (Withdrawn) A computer-readable medium having stored thereon computer executable instructions for performing acts of:

retrieving a user key associated with a first user of a plurality of users from a data structure comprising a plurality of user keys, each user key comprising a master key encrypted using a password associated with a unique one of the plurality of users;

decrypting the retrieved user key using a password associated with the first user to produce a master key; and

accessing data using the master key.

73. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the user key is retrieved using a user id associated with the first user.

74. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key

pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users.

75. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the data structure comprises a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key associated with the one of the plurality of users, and wherein the user key is retrieved using a user id associated with the first user.

76. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the act of decrypting the user key comprises decrypting the user key using a hash of the password associated with the first user.

77. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user to produce a hash value; and

using the hash value as a decryption key to decrypt the user key.

78. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a one-way hash function; and

using the result of the one-way hash function as a decryption key to decrypt the user key.

79. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the act of decrypting the retrieved user key comprises:

hashing the password associated with the first user using a cryptographic hash function; and

using the result of the cryptographic hash function as a decryption key to decrypt the user key.

80. (Withdrawn) A computer-readable medium as recited in claim 72, wherein each of the plurality of user key includes a data verification feature.

81. (Withdrawn) A computer-readable medium as recited in claim 72 having further computer executable instructions for performing acts of:

verifying the integrity of the retrieved user key.

82. (Withdrawn) A computer-readable medium as recited in claim 72, wherein the retrieved user key includes an integrity verification feature and wherein the method further comprises verifying the integrity of the retrieved user key using the integrity verification feature.

83. **(Withdrawn)** A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a checksum and wherein the method further comprises verifying the integrity of the retrieved user key using the checksum.

84. **(Withdrawn)** A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the message authentication code.

85. **(Withdrawn)** A computer-readable medium as recited in claim 72, wherein the retrieved user key includes a keyed-hash message authentication code and wherein the method further comprises verifying the integrity of the retrieved user key using the keyed-hash message authentication code.